SOLUTION BRIEF

DDoS Protection for Colocation, Hosting and Data Center Providers

Overview

The pandemic has raised the bar for colocation, hosting, and data center providers. Enterprise customers and tenants now expect exceedingly high resiliency, reliability, and security as they redistribute their networks between private and public clouds, support a more remote workforce and grow to meet soaring consumer demand for at-home entertainment such as gaming and gambling. IP traffic has increased more than 10 times in the last 10 years and data center storage skyrocketed by a factor of twenty-five.

The threat landscape has also evolved, and cybercriminals have raised the bar too.

DDoS attack sophistication, volume and frequency have increased every year. DDoS attacks can target both the data center infrastructure, impacting large numbers of tenants through service outages or impaired service quality, and specific tenants, with collateral damage on others. In addition, geopolitical events have demonstrated the efficacy of both state-sponsored and grass roots cybercriminals in launching politically motivated DDoS attacks against critical infrastructure and government agencies. Besides common volumetric attacks, cybercriminals can weave DDoS attacks as smokescreens for ransomware, malware, and other techniques to target your most valuable customers.

Service outages and downtime lead to lost revenue. Unsatisfied customers increase churn and raise operational

Challenge

Data center operators are experiencing increasing levels of DDoS attacks to the data center infrastructure and to their enterprise customers/tenants, threatening service availability, revenue, and brand. Limited resources and outdated DDoS mitigation and detection technology is often inadequate for today's threats or to meet higher requirements from customers.

Solution

- Thunder Threat Protection System (TPS)
- aGalaxy® management system
- Surgical, multi-vector DDoS mitigation and detection
- Automated, zero-day defense
- Multi-tenant management and subscriber portal

Benefits

- High service availability
- Reduced security OPEX
- Increased management visibility
- Increased revenue
- Ability to offer more customized or tiered protection services

and marketing expenses to retain and attract new customers. Most importantly, however, it damages the data center's brand and reputation. Your customers can lose over $1M with any outage, according to a recent Uptime Institute report. If you cannot protect them adequately and keep their services up and running in the event of a DDoS attack, they will find someone who can.

For data center operators, the strategies that worked for protecting their own infrastructure may not have the flexibility, granularity, or scale to protect individual tenants profitably. The DDoS protection may not have kept up with the growth in threats and the higher expectations of tenants/customers—an oversight with potentially devastating consequences.

DDoS protection is business critical.

The Challenge

Today's Threats Require Constant Vigilance

For cybercriminals, DDoS attacks have become easier and less expensive to launch, allowing them to increase the frequency, velocity, duration, and complexity of attacks. DDoS attacks are increasingly sophisticated through the combined use of volumetric and application-layer attacks on network bandwidth, server sockets, web server threads and CPU utilization.

The increased deployment of lightly protected IoT devices globally provide a rich recruitment base for growing botnets that target infrastructure worldwide. The DDoS weapons in these botnets have more than doubled in the last few years. A single, compromised server can launch an effective DDoS attack in less than 26 seconds and will actively seek out nearby hosts to compromise. Fast detection and mitigation of early-stage attacks and zero-day tactics will limit attack damage and spread.

Limited Resources Cannot Manage Increasing Traffic and Threats

DDoS attackers have evolved and now use multi-vector attack techniques tuned for their victims. Data center providers have a small staff that must support increasing customer traffic with growth rising sharply due to digital transformation trends. Limited security personnel are stretched to combat growing sophisticated, volumetric DDoS attacks against the data center infrastructure while simultaneously meeting the protection demands of customers.

Data center operators must rethink how to protect their own infrastructure as well as that of their customers/tenants. They must build scalable, profitable DDoS defenses that can surgically distinguish an attacker from a legitimate user for thousands of different customers. Automation, machine learning and high scalability are essential for building profitable, differentiated tiered protection services.

DDoS Attacks Threaten Business Success

Continuous availability is paramount for business success of data center providers and their customers. As the world becomes more depended on IT services, executive management and governments are increasingly concerned about resiliency. Customers will scrutinize reliability very carefully and require further improvements and tighten SLAs.

When not mitigated quickly, DDoS attacks impair or deny mission-critical services for an individual enterprise or, when targeting the data center facilities themselves, all tenants of that facility. Uptime Institute reports that the cost of data center outages has been steadily increasing in recent years, with 15 percent of those surveyed estimating costs of a single outage to exceed one million dollars.

Loss or impairment of service availability from DDoS attacks can cause significant customer dissatisfaction and lead to higher churn, lost revenue, and reputation damage for the data center provider. Underinvestment in DDoS protection infrastructure can create opportunity loss as well, as leading data center providers gain competitive advantage by offering value-added DDoS protection services to their customers in an increasingly competitive market.

A10 Thunder TPS - DDoS Protection Solution

Deploy a scalable, high-performance solution at the data center's edge to protect customers' lower speed downstream links and servers. A10 Networks Thunder TPS mitigates DDoS risks by providing high-performance, network-wide protection against DDoS attacks. It also enables service availability against a variety of volumetric and more sophisticated application attacks. The A10 defenses are fully automated solutions that leverage machine learning with intelligent automation to mitigate DDoS attacks with no manual intervention

Thunder TPS provides the context, packet level granularity and visibility needed to thwart today's sophisticated DDoS attacks. Thunder TPS' scale and zero-touch intelligent automation architecture with aGalaxy management interface maximize ROI and enable profitable DDoS protection services.

Features and Benefits

A10 Thunder TPS is the world's highest-performance DDoS mitigation and detection solution, leading the industry in precision, intelligent automation, scalability, and performance.

A10 Thunder TPS defenses are comprised of these key components: Thunder TPS, Thunder TPS detector and aGalaxy centralized management system. These components are deployed modularly and can scale to meet the demands of any network environment, including global, multi-location data center provider networks.

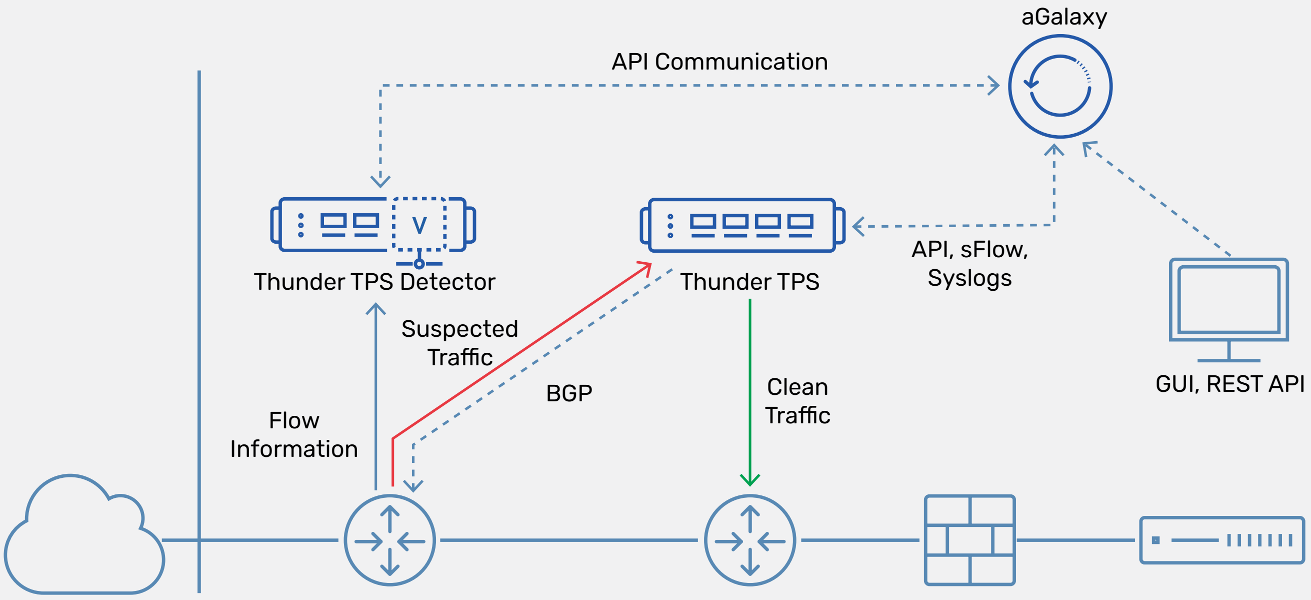

Figure 1: Reactive Deployment for on-demand mitigation in large networks

Thunder TPS Provides:

- **Surgical Multi-Vector DDoS Protection:** Detect and mitigate DDoS attacks of multiple types, including volumetric, protocol, or resource attacks: application-level attacks or IoT-based attacks.
- **ZAP – Zero-Day Automated Protection:** The ZAP engine utilizes heuristic and machine learning to automatically discover mitigation filters without advanced configuration or manual intervention. ZAP speeds the response time against increasingly sophisticated multi-vector attacks while minimizing downtime and errors and lower operating costs.
- **Higher Service Availability:** Thunder TPS ensures service availability by automatically spotting anomalies across the traffic spectrum and mitigating multi-vector DDoS attacks.
- **Scalable Protection:** Thunder TPS hardware models hardware-optimized packet-processing for highly scalable flow distribution and hardware DDoS protection capabilities.
- **Reduced Security OPEX:** Thunder TPS delivers high performance in a small form factor to reduce OPEX with significantly lower power usage, rack space, and cooling requirements.
- **Management Interface:** Thunder TPS supports an industry-standard CLI, on-box GUI, and the aGalaxy management system. The CLI allows sophisticated operators easy troubleshooting and debugging. The intuitive on-box GUI enables ease of use and basic graphical reporting. aGalaxy offers a comprehensive dashboard with advanced reporting, mitigation console, and policy enforcement for multiple Thunder TPS devices, including a partitioned subscriber portal for each customer.

Summary

DDoS Mitigation for Data Center Operators

A10 provides a highly scalable, highly configurable DDoS mitigation solution for data center operators trying to maintain the integrity of their facility or provide advanced protection for their tenants and customers. Thunder TPS helps analyze traffic with ultra-low latency and provides comprehensive tools that minimize outages. Deployed by Tier 1 operators and top gaming companies, A10 has the market proven expertise to meet your needs

Next Steps

To learn more about the A10 Thunder TPS, please contact your A10 representative or visit: a10networks.com/products/thunder-tps/.

About A10 Networks

A10 Networks provides security and infrastructure solutions for on-premises, hybrid cloud, and edge-cloud environments. Our 7000+ customers span global large enterprises and communications, cloud and web service providers who must provide business-critical applications and networks that are secure, available, and efficient. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally. For more information, visit A10networks.com and follow us @A10Networks.

Learn More

About A10 Networks

Contact Us
A10networks.com/contact

Part Number: A10-SB-19140-EN-04 May 2022